統合セキュリティ人材モデル

人材像	説明
【CT】セキュリティコンサルタント	セキュリティエンジニアリングの上流に位置し、経営課題や業務要件から、セキュリティに関するシステム仕様や運用仕様の方針を策定する。
【PL】セキュアシステムプランナー	求められるセキュリティ要件を満たすシステムやアプリケーションの上流設計を担当する。対象領域は、システムアーキテクチャー、ネットワーク、サーバ、アプリケーション、データベースなど。
【DV】セキュアシステムデベロッパー	セキュアシステムプランナーのアウトプットを引き継ぎ、セキュリティ要件を満たすシステム基盤の開発を担当する。対象領域は、システムアーキテクチャー、ネットワーク、サーバ、データベースなど。
【AD】セキュアアプリケーションデベロッパー	セキュアシステムプランナーのアウトプットを引き継ぎ、セキュリティ要件を満たすアプリケーションの開発を担当する。対象領域はアプリケーション、データベースアクセスなど。
【MG】セキュリティマネージャー	ISMSに代表されるセキュリティマネジメントシステムの整備および運用を担当する。
【AU】セキュリティオーディター	ISMSに代表されるセキュリティマネジメントシステムのマネジメント監査を担当する。
【SR】システムリスクアセッサー	対象のICTシステムが直面するセキュリティリスクを分析し、適切なセキュリティ対策選択の指針を示す。
【PT】ペネトレーションテスター	対象のICTシステムに対して攻撃者視点で攻撃を試み、ICTシステムの弱点（脆弱性や危険性等）を把握し報告する。
【NR】ネットワークリスクアセッサー	対象のICTシステムが直面するセキュリティリスクを分析し、適切なセキュリティ対策選択の指針を示す。
【RE】リサーチャー	セキュリティ技術に関する各種の研究を行う。
【FE】フォレンジックエンジニア	セキュリティインシデント発生時に、コンピュータ・フォレンジックプロセスに基づく詳細な調査を実施する。すでに侵害されたディスクイメージなどを採取し、また取得したイメージなどを解析し、攻撃者によっていつどのようなことが行われたのか解析を実施する。
【IA】インテリジェンスアナリスト	セキュリティに関する外部情報を収集・分析し、ICTシステムへの影響度を把握する。また、インシデント発生時にその背景などを分析し、インシデントの重大性に対する判断材料を提供する。
【IR】インシデントレスポンダー	セキュリティインシデントへの１次対処を行う。必要に応じて、インシデントハンドラーなどの他の人材像へのエスカレーション・引継ぎを行う。
【SP】セキュリティオペレーター	ICTシステムのセキュリティに関連する運用を担当する。